UNITED STATES DISTRICT COURT

JAN 19 2023

for the

Eastern District of Missouri

In the Matter of the Seizure of
Approximately $397,674.32 held in [redacted] accounts, further described in Attachment A

Case No. 4:23-MJ-7026-SPM

APPLICATION AND AFFIDAVIT FOR SEIZURE WARRANT

I, [redacted], being duly sworn depose and say:

I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that there is now certain property namely

Approximately $397,674.32 held in [redacted] accounts, further described in Attachment A

which is

subject to forfeiture under Title 18, United States Code, Sections 981(a) and 982(a) and Title 28, United States Code, Section 2461, and therefore, is subject to seizure under Title 18, United States Code, Sections 981(b)& 982(b) and Title 21, United States Code, Sections 853(e)&(f) concerning a violation of Title 18, United States Code, Section 1956 and Title 50, United States Code, Section 1705.

Because the violation giving rise to this forfeiture occurred within the Eastern District of Missouri, this Court is empowered by 18 U.S.C. § 981(b)(3) and 28 USC § 1355(d) to issue a seizure warrant which may be executed in any district in which the property is found. The seized property is to be returned to this district pursuant to 28 U.S.C. § 1355(d).

The funds identified herein are subject to civil forfeiture without regard to their traceability to criminal activity because they are contained in an account into which identical traceable property has been deposited and therefore may be forfeited as fungible property under Title 18, United States Code, Section 984.

The facts to support a finding of Probable Cause for issuance of a Seizure Warrant are as follows:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

Continued on the attached sheet and made a part hereof. X **Yes** ____ **No**

[redacted]

Signature of Affiant, Special Agent [redacted]

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41

January 19, 2023
Date and Time Issued

at St. Louis, Missouri
City and State

Honorable Shirley P. Mensah, U.S. Magistrate Judge
Name and Title of Judicial Officer

[redacted]

Signature of Judicial Officer

AFFIDAVIT IN SUPPORT AN APPLICATION FOR SEIZURE WARRANT

I, [redacted] a Special Agent with the Federal Bureau of Investigation ("FBI"), being duly sworn, depose and state as follows:

1. I am a Special Agent at the Federal Bureau of Investigation ("FBI"). I have been a Special Agent with the FBI since [redacted] 2007. Since April 5, 2010, I have been assigned to a cyber squad in the FBI's St. Louis Field Office. I have received training regarding computer fraud and computer hacking. I have conducted investigations into various forms of online criminal activity and am familiar with the ways in which such crimes are commonly conducted. In addition, I have participated in the execution of search warrants involving electronic evidence.

2. The facts set forth in this affidavit are based on my personal knowledge, the knowledge obtained during my participation in this investigation, the knowledge obtained from other individuals, including other law enforcement personnel, review of documents and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience.

3. This affidavit does not contain all of the information known to me in regard to the investigation; however, it contains information establishing probable cause to seize approximately $397,674.32 held in the specific [redacted] accounts listed in Attachment A (the "**Target Accounts**"). [redacted] is a U.S.-based financial services company that provides online money transfer and digital payment services to its customers, who can use their [redacted] account to receive, store, and send money, including to counterparties from outside of the [redacted] network.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that unknown foreign persons have committed violations of 50 U.S.C. § 1705(a) (International Emergency Economic Powers Act, or "IEEPA") and 18 U.S.C. § 1956 (money laundering) (the "Subject Offenses"). This includes performing online freelance information technology work for North Korea in violation of IEEPA. There is probable cause to seize the funds in the **Target Accounts** as proceeds traceable to IEEPA violations, and as property involved in money laundering violations, or traceable to such property.

APPLICABLE STATUTES

A. International Emergency Economic Powers Act (IEEPA)

5. Under IEEPA, it is a crime to willfully violate or conspire to violate any license, order, regulation, or prohibition issued pursuant to IEEPA, including restrictions imposed by the Department of Treasury. 50 U.S.C. § 1705(a).

6. The Department of Treasury's Office of Foreign Asset Control (OFAC) has the authority to designate for sanctions entities or people determined to have violated the President's Executive Orders.

7. On September 13, 2018, OFAC designated for sanctions a North Korean information technology firm based in China named Yanbian Silverstar Network Technology Co., Ltd ("Yanbian Silverstar"), as well its Russia-based front company, Volasys Silver Star, for violating the President's Executive Orders. These entities exported workers from North Korea to generate revenue for the Government of North Korea (in violation of Executive Order 13722), and employed North Korean workers in the information technology industry (in violation of Executive Order 13810). The same OFAC designation also included a North Korean national, [redacted], identified by OFAC as the CEO of Yanbian Silverstar and Volasys Silver Star.

8. According to the OFAC designation press release, the sanctioned parties had channeled "illicit revenue to North Korea from overseas information technology workers disguising their true identities and hiding behind front companies, aliases, and third-party nationals." In other words, the sanctioned parties were conspiring to create and use pseudonymous email accounts, social media accounts, payment platform accounts, and online job site accounts to obfuscate their true identities as North Koreans, and to solicit and perform information technology freelance jobs to earn money for the North Korean government in violation of U.S. sanctions.

B. Money Laundering

9. 18 U.S.C. § 1956(h) criminalizes a conspiracy to commit money laundering.

10. 18 U.S.C. § 1956(a)(1)(B)(i) criminalizes conducting, or attempting to conduct, a financial transaction which involves the proceeds of specified unlawful activity, knowing that the property involved in such financial transaction represents the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of said specified unlawful activity.

11. Under 18 U.S.C. § 1956(c)(7)(D), the term "specified unlawful activity" includes violations of IEEPA. The financial transactions described in this affidavit are overt acts in furtherance of a money laundering conspiracy to conceal IEEPA violations.

C. Forfeiture

12. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property which constitutes or is derived from proceeds traceable to a violation of IEEPA, is subject to criminal and civil forfeiture.

13. Property involved in a money laundering offense is subject to forfeiture under both civil and criminal forfeiture authorities. Pursuant to 18 U.S.C. § 981(a)(1)(A), any property, real or personal, involved in a transaction or attempted transaction in violation of 18 U.S.C. § 1956, or any property traceable to such property, is subject to civil forfeiture. In addition, pursuant to 18 U.S.C. § 982(a)(1), any property involved in a violation of 18 U.S.C. § 1956, or any property traceable to such property, is subject to criminal forfeiture. Forfeiture pursuant to these statutes applies to more than just the proceeds of the crime. These forfeitures encompass all property "involved in" the crime, which can include untainted funds that are comingled with tainted funds derived from illicit sources.

14. Pursuant to 18 U.S.C. § 981(b), property subject to civil forfeiture may be seized by a civil seizure warrant issued by a judicial officer "in any district in which a forfeiture action against the property may be filed," and may be executed "in any district in which the property is found," if there is probable cause to believe the property is subject to forfeiture. A civil forfeiture action may be brought in any district where "acts or omissions giving rise to the forfeiture occurred." 28 U.S.C. § 1355(b)(1)(A). As detailed below, acts in furtherance of the fraud and money laundering scheme under investigation occurred in the Eastern District of Missouri. The criminal forfeiture statute, 18 U.S.C. § 982(b)(1), incorporates the procedures in 21 U.S.C. § 853, which provides authority for the issuance of a seizure warrant for property subject to criminal forfeiture.

15. 18 U.S.C. § 984 allows the United States to seize for civil forfeiture identical substitute property found in the same place where the "guilty" property had been kept. For purposes of Section 984, this affidavit need not demonstrate that the funds now in the **Target Accounts** are the particular funds involved in the fraud and money laundering violations, so long

as the forfeiture is sought for other funds on deposit in that same account. Section 984 applies to civil forfeiture actions commenced within one year from the date of the offense.

16. Based on the foregoing, the issuance of this seizure warrant is authorized under 21 U.S.C. § 853(f) and 18 U.S.C. § 982(b)(1) for criminal forfeiture; and 18 U.S.C. §§ 981(b) and 984 for civil forfeiture. Notwithstanding the provisions of Rule 41(a) of the Federal Rules of Criminal Procedure, the issuance of this seizure warrant in this district is appropriate under 18 U.S.C. § 981(b)(3) and 28 U.S.C. § 1355(b)(1) because acts or omissions giving rise to the forfeiture occurred in the Eastern District of Missouri.

BACKGROUND REGARDING NORTH KOREAN INFORMATION TECHNOLOGY WORKERS

17. According to a May 16, 2022, report jointly issued by the U.S. Department of State, Department of Treasury, and the FBI, North Korea uses freelance information technology workers to generate a revenue and foreign currency stream for its weapons of mass destruction and ballistic missile programs.

18. Because this work violates U.S. sanctions, the freelance North Korean IT workers deceive their employers by buying, stealing, or counterfeiting the identities and mailing addresses of non-North Koreans when bidding on and completing freelance projects, in order to conceal their identities as North Koreans.

19. North Korean IT workers also either pay or deceive non-North Koreans to interview for jobs for them, accept payment for freelance projects, and videoconference with their employers when necessary. These non-North Koreans may not be aware that the IT workers are North Korean.

20. North Korean IT workers use multiple accounts and multiple freelance contracting platforms, digital payment platforms, social media and networking applications, and

email and messaging applications, in order to obtain and perform IT contracts, receive payment for their work, and launder those funds.

21. The North Korean IT workers are primarily located in China and Russia. In order to avoid suspicion that they are North Korean and be able to use U.S.-based online services, North Korean IT workers use virtual private networks, virtual private servers, and proxy IP addresses to appear that they are connecting to the internet from false locations. North Korean IT workers also use remote desktop software to access U.S.-based computers to appear that they are connecting to online services from false locations.

FACTS ESTABLISHING PROBABLE CAUSE TO BELIEVE CRIMES HAVE BEEN COMMITTED

22. In August 2019, the FBI interviewed an individual located in the United States ("Individual 1") who had an account at [redacted] is a global freelancing platform based in the United States, which serves as an online marketplace where businesses advertise for independent professionals or freelance workers, who in turn can find work in a variety of industries, including software development and information technology.

23. Individual 1 described communications with another individual who has been using the [redacted] account [redacted] and the telephone number [redacted]. This second individual is referred to as [redacted].

24. Individual 1 allowed [redacted] to use Individual 1's [redacted] account for freelance work. Individual 1 also agreed to purchase a laptop for [redacted] and keep it in Individual 1's home in the United States. Individual 1 told the FBI that [redacted] used remote access software to use the computer located in Individual 1's residence, and that the computer's monitor showed that the remote user was using the computer for [redacted] Individual 1 eventually had four laptops used by [redacted] with [redacted] paying Individual 1 $100

per month per laptop.

25. [redacted] also requested that Individual 1 find other people with additional [redacted] accounts that [redacted] could use, but Individual 1 did not refer any people to [redacted].

26. For the work completed by [redacted] through Individual 1's [redacted] account, the payments would be channeled through Individual 1's [redacted] account and sent (minus a portion of the money kept by Individual 1) to [redacted] using his accounts at the payment platforms [redacted].

27. According to Microsoft, the [redacted] account [redacted] used by Individual 1 to contact [redacted] was registered with the email address [redacted]@yandex.com. Yandex.com is a Russian email provider.

28. According to [redacted] an account was registered with the telephone number [redacted], which had been used by Individual 1 to contact [redacted] and the email address [redacted]@gmail.com, and the answer to the security question is "[redacted]."

29. According to [redacted] the separate account used by [redacted] to receive payment from Individual 1 for freelance work was registered using the email address [redacted]@126.com (126.com is a Chinese email provider), and the answer to the security question was [redacted]," which is Chinese for Silver Star. According to [redacted] this account used by [redacted] to receive payment from Individual 1 for freelance work received over $85,000 between April 2018 and October 2019.

30. Based on my training and experience, the use of a Chinese email provider and security question, the similarity of the security question to the name of the sanctioned North Korean IT worker front company Yanbian Silverstar, the receipt of funds, and the use of an

intermediary's [redacted] account, multiple [redacted] accounts, multiple email accounts, and a U.S.-based laptop to conduct freelance IT work, I have probable cause to believe that [redacted] is a North Korean IT worker living in China and working at Yanbian Silverstar.

31. Through an approved undercover operation, the FBI utilized an online undercover employee ("OCE") to communicate while in the Eastern District of Missouri via [redacted] with [redacted]. In August 2020, [redacted] explained his need for a U.S. [redacted] account and that he would pay 15% of the monthly earnings to the OCE for the use of the account. Also, [redacted] needed a laptop so he could connect via a remote desktop-type application. This would provide [redacted] with the appearance of residing in the United States and the ability to avoid using a Virtual Private Network ("VPN") IP address, which might be blocked by [redacted] On August 16, 2020, [redacted] agreed to provide $75 to the OCE to purchase a laptop. On August 17, 2020, OCE received the $75 payment from a [redacted] account registered with email address [redacted]@126.com.

32. According to [redacted] the account used by [redacted] to receive payment from Individual 1 for freelance work logged on from IP address 36.97.143.26 ("IP Address 1") from April 27, 2018, to October 13, 2019. Based on databases regularly relied upon by the FBI, IP Address 1 resolves to China Telecom, Jilin, China and was associated with a dedicated server during this time period. The dedicated server means accounts accessed by IP Address 1 during this time period would have been working together, likely from the same location and for the same organization.

33. Based on my training and experience, and evidence of a North Korean IT worker living in China and working at Yanbian Silverstar using a Chinese dedicated server located at IP Address 1 to access [redacted] I have probable cause to believe that others using IP Address 1

between April 27, 2018, to October 13, 2019, are also North Korean IT workers living in China and working at Yanbian Silverstar.

34. According to [redacted] there were 64 [redacted] accounts that were created or accessed from IP Address 1 between April 27, 2018, to October 13, 2019. Many contained the name "Silver Star" in their subscriber information and indicated that the users' location was in Jilin, China, corroborating that the users of IP Address 1 are North Korean IT workers living in China and working at Yanbian Silverstar. For example, one of these [redacted] accounts listed the business name "Yanbian Silver Star Network Technology Co., Ltd.," and an address in Jilin, China.

35. The FBI's review of the account information for these [redacted] accounts showed payments from freelancer platforms such as [redacted]. Many [redacted] accounts also listed multiple email addresses in their subscriber information (allowing the user to register numerous freelancer platform accounts with the same [redacted] account). These characteristics corroborate the probable cause that these accounts are used by North Korean IT workers living in China and working at Yanbian Silverstar.

36. In February and July, 2022, United States Magistrate Judges Shirley P. Mensah and John M. Bodenhausen in the Eastern District of Missouri signed federal search warrants for numerous Google and Microsoft for accounts associated to Yanbian Silverstar actors based on the information received from [redacted] The communications from these Google and Microsoft accounts discussed using identities of third parties to open accounts at payment and freelancer platforms. They also used Korean language and North Korean honorifics to communicate with each other. Those communications clearly identified them as North Koreans doing IT work on behalf of North Korea.

37. A review of the records from the Google and Microsoft search warrants identified

additional email accounts, bank accounts, telephone numbers, fictitious company names, and stolen personally identifiable information (PII), such as SSN, date of birth, and address, used by the Yanbian Silverstar actors to create their online payment and freelancer platform accounts.

38. In June 2022, United States Magistrate Judge Stephen R. Welby in the Eastern District of Missouri signed a federal search warrant for several Slack groups and channels associated to Yanbian Silverstar actors based on the review of the Google and Microsoft accounts. Slack is a communication platform used by freelance and developers to communicate and share files with their team remotely. The communications in these accounts discussed using identities of third parties to open accounts at payment and freelancer platforms. They also used Korean language and North Korean honorifics to communicate with each other. Those communications clearly identified them as North Koreans doing IT work on behalf of North Korea. Several of the [redacted] accounts shared China bank account information, China National ID cards, email addresses, and payment requests. Additionally, the [redacted] included the use of North Korean names and job titles associated to Yanbian Silverstar and Volasys Silver Star leadership and IT workers.

39. The email addresses and financial identifiers associated with Yanbian Silverstar, provided by [redacted], Microsoft, Google, and Slack Technologies were in turn provided to [redacted] provided a list of accounts matching those identifiers. The general pattern of these accounts includes physical addresses in China, payments received from freelancer and payment platforms, and withdrawals of funds to accounts at Chinese banks. I know from my training and experience that North Korean IT workers frequently use China-based banks to spend their freelancer revenue or else transmit it to North Korea.

40. In October 2022, United States Magistrate Judge John M. Bodenhausen in the

Eastern District of Missouri signed a federal seizure for 44 [redacted] accounts. The majority of the accounts were identified by the FBI from a review of previous search warrants on IT worker controlled accounts. The remaining accounts were identified by [redacted] fraud detection unit based on connections and similar patterns of activity to the FBI identified accounts. All of the accounts were independently corroborated by the FBI as being controlled by North Korean IT workers. The FBI conducted an additional review of the search warrant records from Google, Microsoft, and Slack and identified additional [redacted] accounts controlled by North Korean IT workers.

41. The FBI conducted analysis of the [redacted] accounts identified, and a subset of those accounts are the funds in the **Target Accounts** to be seized in Attachment A.

42. The Target Accounts, which comprise 35 [redacted] accounts holding $397,674.32 in proceeds from the fraud scheme, are further described below. These are accounts provided by [redacted] using identifiers associated with Yanbian Silverstar and Volasys Silver Star, which had a remaining balance as of the date of this application, and which were then confirmed by the FBI as being used by North Korean IT workers. The subscriber information listed below for each account was provided by the subscriber to [redacted]

a. [redacted] Cardholder ID: 34661348 has an outstanding balance of $60,000 with the following account information:

Name: [redacted]

Registration Date: 10/29/2019

i. During the period of November 2019 to December 2022, the account received $726,867.42 from other [redacted] accounts, sent $126,924.58 to

other [redacted] accounts, and withdrew a total of $544,945.02 to a bank account in China. This money movement is consistent with an account used by North Korean IT workers to launder money.

ii. The [redacted] account for email address [redacted]@126.com used China National ID number [redacted]0225 along with a picture of an ID to open the account. The same China National ID number was used on the bank account associated to the [redacted] account for email address [redacted]@126.com. This [redacted] account was one of the seized accounts in the seizure warrant from October 2022 and was discussed in paragraph 29. The use of the same China National ID to open this account and on a China bank account for another North Korean [redacted] account demonstrates both accounts are controlled by North Korean IT workers.

iii. The [redacted] account with email address [redacted]@126.com received a total of $299,000 from August 2022 to December 2022 in $20,000 amounts, with the exception of one $19,000 transfer, from the [redacted] account with email address [redacted]@126.com, which is discussed further below. Additionally, the account received a total of $224,000 from May 2022 to December 2022 in $20,000 amounts, with the exception of a $19,000 and $25,000 transfers, from the [redacted] account with email address [redacted]@126.com, which is also discussed further below. The transfer of similar amounts over a short time to other North Korean IT worker controlled accounts further corroborates the [redacted] account is controlled by North Korean IT workers.

b. [redacted] Cardholder ID: 48539184 has an outstanding balance of $50,876.63 with the following account information:

Name: [redacted]
Registration Date: 12/9/2021

i. During the period of December 2021 to October 2022, the account received $520,584.61 from other [redacted] accounts, sent $293,982.67 to other [redacted] accounts, and withdrew a total of $720,000 to a bank account in China. This money movement is consistent with an account used by North Korean IT workers to launder money.

ii. A review of the documents provided by the customer to [redacted] identified an invoice dated April 2, 2022, which had the name [redacted] and email address [redacted]@gmail.com. The email address [redacted]@gmail.com used the recovery account of [redacted]@gmail.com, an account previously searched by the FBI, and has been identified as being used by [redacted] North Korean IT worker. Because the North Korean user of the recovery address also has access to the email address provided to [redacted] the FBI has probable cause to believe the same North Korean IT worker controls the [redacted] account to be seized.

iii. According to [redacted] records from Microsoft, in January 2022, the email address [redacted]@126.com and its password was shared between the two [redacted] accounts ([redacted] and [redacted]) controlled by

[redacted], the Company President of Yanbian Silverstar. The sharing of the email address and control of the email password used to register the [redacted] account corroborates the [redacted] account is controlled by North Korean IT workers.

c. [redacted] Cardholder ID: 40408285 has an outstanding balance of $182 with the following account information:

Name: [redacted]
Registration Date: 10/12/2020

i. During the period of December 2020 to November 2022, the account received $1,934,976.45 from other [redacted] accounts, sent $425,911.40 to other [redacted] accounts, and withdrew a total of $1,865,505.01 to a bank account in China.

ii. According to [redacted] records, in December 2020, the email address [redacted]@126.com was provided to [redacted] (using the [redacted] username [redacted] from delegation leader [redacted] (using the [redacted] username [redacted]) in Korean-language [redacted] about freelance IT work, and stated it was a [redacted] address. The sharing of the [redacted] email address between the Company President and a Delegation Leader demonstrates the [redacted] account is controlled by North Korean IT workers.

d. [redacted] Cardholder ID: 38065868 has an outstanding balance of $37,368.93 with the following account information:

Name: [redacted]

[redacted]
Registration Date: 5/28/2020

i. During the period of June 2020 to August 2021, the account received $1,180,242.29 from other [redacted] accounts, sent $22,425.34 to other [redacted] accounts, and withdrew a total of $1,160,300.00 to a bank account in China.

ii. According to [redacted] records, in June 2020, the email address [redacted]@126.com and its password was shared between the two [redacted] accounts ([redacted]) controlled by [redacted], the Company President of Yanbian Silverstar. The sharing of the email and password demonstrates the account is controlled by North Korean IT workers.

e. [redacted] Cardholder ID: 47630229 has an outstanding balance of $33,024.13 with the following account information:

Name: [redacted]
Registration Date: 10/27/2021

i. During the period of November 2021 to November 2022, the account received $46,434.38 from other [redacted] accounts, sent $531,978.21 to other [redacted] accounts, and withdrew a total of $35,050 to a bank account in China.

ii. According to [redacted] records, in January 2022, the email address [redacted]@126.com and its password was shared between the two [redacted] accounts ([redacted]) controlled by

[redacted], the Company President of Yanbian Silverstar. The sharing of the email and password demonstrates the [redacted] account is controlled by North Korean IT workers.

f. [redacted] Cardholder ID: 42388706 has an outstanding balance of $23,920.60 with the following account information:

Name: [redacted]
Registration Date: 02/07/2021

i. During the period of May 2021 to June 2022, the account received $98,100 from other [redacted] accounts and sent $119,849 to other [redacted] accounts, and withdrew a total of $17,850 to a bank account in China.

ii. The [redacted] account with email address [redacted]@163.com sent two payments for $16,500 and $19,600 in February and March 2022 to the [redacted] account with email address [redacted]@163.com, which discussed further below. The similar naming convention of the email addresses, using the initials of their name and their date of births, as well as the same China-based email provider, demonstrates the accounts were more than likely created by the same person. Additionally, the transfer of money to another North Korean IT worker controlled account further corroborates the [redacted] account is controlled by North Korean IT workers.

iii. The [redacted] account [redacted]@163.com was registered from IP address 124.94.6.194 on February 7, 2021 and resolves to China Unicom. Another [redacted] account using the email address [redacted]@163.com and the name "[redacted]", which discussed further below, logged in from the same IP address on February 5, 2021. The logins from the same IP address, similar email naming convention, and the use of "[redacted]" further corroborates that the account was likely controlled by the same individual(s).

g. [redacted] Cardholder ID: 23163213 has an outstanding balance of $19,018.68 with the following account information:

Name: [redacted]
Registration Date: 08/10/2017

i. During the period of September 2017 to October 2021, the account received $3,368,697.86 from other [redacted] accounts and sent $313,237.78 to other [redacted] accounts, and withdrew a total of $4,071,269.02 to a bank account in China.

ii. According to [redacted] records, on or about December 10, 2020, [redacted] user [redacted] sent a screenshot of a $20,000 USD withdrawal from [redacted] to a bank account ending in #8277 to [redacted] user [redacted] which your affiant knows to be used by [redacted], the Company President of Yanbian Silverstar. In the [redacted] records, [redacted] asked about the email address associated to the account and [redacted] provided the email address [redacted]@gmail.com. A review of [redacted]

for the account identified a $20,000 withdrawal on 12/10/2020.

iii. A review of the documents provided by the customer to [redacted] identified a China National Identification card with the number [redacted]. According to [redacted] records, in August 2017, a picture with the same China National Identification card was shared from [redacted] account [redacted], used by [redacted], the Company President of Yanbian Silverstar, to [redacted] used by [redacted]-[redacted], Delegation Leader, Volasys Silver Star. The sharing of the ID card by two North Korean IT worker leaders and its use to open a [redacted] account demonstrates the [redacted] account is controlled by North Korean IT workers.

h. [redacted] Cardholder ID: 56502641 has an outstanding balance of $18,075 with the following account information:

Name: [redacted]
Registration Date: 08/09/2022

i. During the period of August 2022 to December 2022, the account received $99,275 from other [redacted] accounts and withdrew a total of $81,200 to a bank account in China.

ii. The [redacted] account with email address [redacted]@163.com received four transfers from the [redacted] account using the email address [redacted]@163.com,which is discussed further below. The amounts were for $9,500; $13,000; $14,000; and $7,500. Additionally, the

[redacted] account [redacted]@163.com was created from IP address 113.229.205.208, which resolves to China Unicom, and the [redacted] account [redacted]@163.com logged in from the same IP address on August 10, 2022, one day after this account was created.

iii. The similar naming convention of the email addresses, using the initials of their name and their date of births, the same China based email provider, and login from the same IP address, demonstrates the accounts were more than likely created by the same person. Additionally, the transfer of money to another North Korean IT worker controlled account further corroborates the [redacted] account is controlled by North Korean IT workers.

i. [redacted] Cardholder ID: 47779486 has an outstanding balance of $17,431.24 with the following account information:

Name: [redacted]

Registration Date: 11/4/2021

i. During the period of November 2021 to June 2022, the account received $84,760.00 from other [redacted] accounts, sent $11,520.93 to other [redacted] accounts, received $25,092.16 from [redacted] (which is a San Francisco based human resource and payroll processing company that facilitates payments for companies), and withdrew a total of $80,900 to a bank account in China.

ii. According to [redacted] records from Microsoft, in 2020, [redacted] corresponded in Korean via [redacted] about IT projects with the [redacted]

account registered with the email address [redacted]@gmail.com. According to records from Google, [redacted]@gmail.com accessed North Korea maps and a North Korean news site, the email account was used to apply for IT worker jobs, and the cloud storage contained resumes, job descriptions, interview scripts, and spreadsheets in Korean cataloging monthly revenue of various email addresses. According to records from Slack, the user with the email address [redacted]@gmail.com also operated the channel [redacted]slack.com, which was used for organizing freelance North Korean IT work. A review of this channel identified a message on November 25, 2021, from user [redacted] requesting a payment of $7,250 be sent to [redacted]@163.com for "Payment for development". A screen shot of the [redacted] transaction was sent in response by user [redacted]. A review of the [redacted] records confirmed a payment was sent on November 25, 2021, from [redacted] account [redacted] in the name of [redacted]. North Korean IT workers will frequently pay each for "development" work. This demonstrates that the email address [redacted]@163.com is used for North Korean IT work.

j. [redacted] Cardholder ID: 53718284 has an outstanding balance of $14,031.76 with the following account information:

Name: [redacted]
Registration Date: 6/13/2022

i. During the period of September 2022 to December 2022, the account

received $205,939.64 from other [redacted] accounts, sent $27,387.10 to other [redacted] accounts, received $1,039.22 via ACH from [redacted]. (which is a money transfer service company based in the United States) for suspected freelancer work, and withdrew a total of $165,500 to a bank account in South Korea.

ii. A review of the [redacted] In-Network payments identified that, over the course of two days, the account received 5 payments totaling $40,000 from one [redacted]@126.com, which is discussed above. Another payment was received for $14,000 from [redacted] account [redacted]@126.com, which is a known North Korean IT worker controlled account, whose password was provided to [redacted] (using the [redacted] username [redacted]) from Delegation Leader [redacted] (using the [redacted] username [redacted]). This money movement is consistent with an account used by North Korean IT workers to launder money.

iii. A review of the documents provided by the customer to [redacted] identified a Chinese passport for [redacted] which indicated they were born in Jilin, China, and the passport was issued by the Chinese embassy in South Korea. North Korean IT workers in China, including those in Jilin, utilize Chinese citizens' identities to open financial accounts. While this account utilized a South Korean address and bank, the use of a Chinese passport and citizen indicates the account is still controlled by

North Korean IT workers.

k. [redacted] Cardholder ID: 48542914 has an outstanding balance of $11,221.10 with the following account information:

Name: [redacted]
Registration Date: 12/10/2021

i. During the period of January 2022 to April 2022, the account received $334,256.76 from other [redacted] accounts, sent $23,035.66 to other [redacted] accounts, and withdrew a total of $300,000 to a bank account in China. The account received a total of $100,000 from [redacted] Cardholder ID 27851354, email address [redacted]@126.com, which previously held funds that were seized by the FBI pursuant to a federal seizure warrant in October 2022.

ii. According to [redacted] records, in January 2022, the email address [redacted]@126.com and its password was shared between the two [redacted] accounts ([redacted]) controlled by [redacted], the Company President of Yanbian Silverstar. The sharing of the email and password corroborates the account is controlled by North Korean IT workers.

l. [redacted] Cardholder ID: 44911814 has an outstanding balance of $10,000.10 with the following account information:

Name: [redacted]
Registration Date: 06/21/2021

i. During the period of January 2022 to April 2022, the account received $528,893.31 from other [redacted] accounts, sent $32,919.11 to other [redacted] accounts, and withdrew a total of $539,998.00 to a bank account in China.

ii. According to [redacted] records, [redacted]@gmail.com's [redacted] account was associated with a Chinese bank account in the name of "[redacted]". Another [redacted], [redacted], [redacted]@yahoo.com, had the same bank account information. The [redacted] [redacted] account used the security answers "[redacted]", "[redacted]", and "0120," all of which have been observed being previously used by North Korean IT workers as security answers for other [redacted] accounts. The use of the same bank account demonstrates both accounts are controlled by North Korean IT workers.

m. [redacted] Cardholder ID: 27185130 has an outstanding balance of $9,130 with the following account information:

Name: [redacted]
Registration Date: 6/29/2018

i. During the period of October 2020 to February 2022, the account received $2,708,763.87 from other [redacted] accounts, received $2,645.11 from credit card payments, and withdrew a total of $2,767,819.12 to a bank account in China.

ii. According to [redacted] records, in August 2021, the account [redacted],

used by [redacted], the Company President of Yanbian Silverstar, sent the email address [redacted]@outlook.com to his other [redacted] account, [redacted] frequently shared bank account information, email addresses, and passwords between his two [redacted] accounts. The sharing of the email address by the company president of Yanbian indicates the account is controlled by North Korean IT workers.

iii. The [redacted] account for email address [redacted]@outlook.com used China National ID number [redacted] along with a picture of an ID to open the account. The same China National ID number was used on the bank account associated to the [redacted] account for email address [redacted]@gmail.com, which is discussed further below. The use of the same China National ID to open this account and on a China bank account for another North Korean [redacted] account demonstrates both of these accounts are controlled by North Korean IT workers.

n. [redacted] Cardholder ID: 52324106 has an outstanding balance of $2,259.62 with the following account information:

Name: [redacted]
Registration Date: 05/02/2022

i. During the period of May 2022 to November 2022 the account received $68,737.00 from other [redacted] and sent $138,494.05 to other

[redacted] accounts.

ii. A review of the documents provided by the customer to [redacted] identified a China National Identification card with the number [redacted]. According to [redacted] records, in May 2022, a picture of the same China National Identification card was shared from [redacted] account [redacted], used by [redacted], Delegation Leader, Yanbian Silverstar, to [redacted] account [redacted], used by [redacted]-[redacted], the Company President of Yanbian Silverstar. The sharing of the ID card by two North Korean IT worker leaders and its use to open a [redacted] account demonstrates the account is controlled by North Korean IT workers.

o. [redacted] Cardholder ID: 32838551 has an outstanding balance of $7,232.86 with the following account information:

Name: [redacted]
Registration Date: 07/16/2019

i. During the period of October 2019 to August 2021, the account received $1,056,321.86 from other [redacted] accounts, sent $73,067.00 to other [redacted] accounts, and withdrew a total of $1,080,942.49 to a bank account in China.

ii. According to [redacted] records, in July 2019, the email address [redacted]@126.com and its password was shared between the two [redacted] accounts controlled by [redacted], the Company President of

Yanbian Silverstar, namely, [redacted] The sharing of the email and password demonstrates the account is controlled by North Korean IT workers.

p. [redacted] Cardholder ID: 48724076 has an outstanding balance of $9,740.52 with the following account information:

Name: [redacted]
Registration Date: 12/20/2021

i. During the period of October 2019 to August 2021, the account received $1,056,321.86 from other [redacted] sent $73,067 to other [redacted] accounts, and withdrew a total of $116,258.20 to a bank account in China.

ii. According to [redacted] records, in November 2021, the email address [redacted]@gmail.com and its password was shared between two [redacted] accounts: [redacted] and [redacted] Both accounts communicate in Korean language and discuss payments to developers and from IT freelancer jobs. The sharing of the email and password demonstrates the account is controlled by North Korean IT workers.

q. [redacted] Cardholder ID: 39841566 has an outstanding balance of $14,881.76 with the following account information:

Name: [redacted]
Registration Date: 9/8/2020

i. During the period of October 2020 to December 2022, the account received $19,431 from other [redacted] accounts, sent $624,276.50 to other [redacted] accounts, received $644,692.90 from [redacted] (an online freelance work marketplace) for freelancer work, paid $16,906.14 to freelancer websites (since September 2022), and withdrew a total of $16,400 to an online bank account in the United States.

ii. Based on the large amount of freelancer revenue and payments to other [redacted] accounts, but a small amount of bank withdrawals, the FBI believes [redacted] is allowing a North Korean IT worker to use his [redacted] account to receive payments and [redacted] is receiving a percentage of the earnings. North Korean IT workers typically share a percentage of their earnings with individuals who allow them to utilize their account. Based on the amounts above, [redacted] would have received approximately 2.5% of the North Korean IT workers earnings. Alternatively, the bank account and [redacted] account could be controlled solely by the North Korean IT worker. The U.S. bank used for the withdrawals on the [redacted] account is [redacted] which is an online bank provider and allows accounts to be opened and managed online.

iii. From October 2020 to February 2022, the [redacted] account [redacted]@gmail.com sent $194,442.50 to [redacted] account, [redacted]@126.com, which previously held funds that were seized by the FBI pursuant to a federal seizure warrant in October 2022. A review of records from [redacted] identified the account

[redacted]@126.com submitted an invoice to [redacted] with [redacted] name, address, and email address for "Mobile Dev" for $1,000 on January 14, 2022. A subsequent payment was made from [redacted] account to [redacted] account for $1,000. The FBI believes the invoice and payment were created to give the appearance that the previous $187,442.50 payments sent to the [redacted] account were all for IT work and to conceal the fact that the funds are actually comprised of those earned by North Korean IT workers.

iv. A review of the Global Payment Services (GLPS) Questionnaire answers provided by the user of the [redacted] account listed a [redacted] webpage profile at www[redacted] On or about December 21, 2022, the [redacted] profile for the URL listed was not available. Yet the account was receiving payments from [redacted] from October 26, 2020, to December 15, 2022.

v. Based on the activity and payments to multiple North Korean accounts, the account is believed to be part of the money laundering conspiracy.

r. [redacted] Cardholder ID: 42231644 has an outstanding balance of $6,444.32 with the following account information:

Name: [redacted]
Registration Date: 1/29/2021

i. During the period of September 2021 to November 2022 the account received $9,000 from other [redacted] accounts, sent $249,083.36 to other [redacted] accounts, received $249,000.72 via ACH from various

companies in names other than "[redacted]" for suspected freelancer work, and withdrew a total of $2,473.04 to banks in the United States and United Kingdom.

ii. Based on the large amount of freelancer revenue and payments to other [redacted] accounts, but a small amount of bank withdrawals, the FBI believes [redacted] is allowing a North Korean IT worker to use his [redacted] account to receive payments and [redacted] is receiving a percentage of the earnings. North Korean IT workers typically share a percentage of their earnings with individuals who allow them to utilize their account. Based on the amounts above, [redacted] would have received less than 1% of the North Korean IT workers earnings. Alternatively, the bank accounts and [redacted] account could be controlled solely by the North Korean IT worker. There are 11 bank accounts listed on the [redacted] account, only three of which are in [redacted] name (two of those three accounts use online banking institutions whose accounts can be opened and managed online by anyone with the person's identifiers). The other bank accounts listed were in Israel, the United Kingdom, and the United States. The adding of bank accounts in names other than the [redacted] accountholder, is a technique utilized by North Korean IT workers.

iii. A review of the documents provided by the customer to [redacted] identified a Texas driver license for [redacted]. Based on its appearance the FBI believes it to be a photoshopped driver license containing [redacted]s information. Therefore, the FBI believes a North Korean IT worker

obtained [redacted] information and created the false DL in order to open a [redacted] account.

s. [redacted] Cardholder ID: 36782803 has an outstanding balance of $6,398.23 with the following account information:

Name: [redacted]
Registration Date: 03/16/2020

i. During the period of September 2020 to April 2022, the account received $49,213.00 from other [redacted] accounts, sent $165,733.30 to other [redacted] accounts, and withdrew a total of $45,600 to bank accounts in China and Peru.

ii. According to records from Slack, the user with the email address [redacted]@gmail.com also operated the channel [redacted] slack.com, which identified multiple messages in Korean language from June 2021 to April 2022 where multiple North Korean Slack users listed the email address [redacted]@gmail.com followed by an amount. Several of these messages contained a screenshot of a [redacted] confirmation screen with the same amount in the [redacted] Some of the messages contained the words "development" and "weekly payment". This demonstrates that the email address [redacted]@gmail.com is used for North Korean IT work.

t. [redacted] Cardholder ID: 31740755 has an outstanding balance of $328.65 with the following account information:

Name: [redacted]

Registration Date: 04/23/2019

i. During the period of April 2019 to November 2022, the account received $49,213.00 from other [redacted] accounts, sent $1,698,420.68 to other [redacted] accounts, and $57,539.90 to a bank account in China. The account received $18,058.91 in payments from [redacted] and other freelancer companies. Additionally, the account received a total of $584,001.84 from various [redacted] accounts in the name of [redacted] and from [redacted] (an online money transfer provider) in the name of [redacted].

ii. According to [redacted] records, in May 2020, the email address [redacted].com was provided [redacted] user [redacted] to [redacted] used by [redacted], Company President, Volasys Silver Star. The user provided the date of May 8, 2020, then a Korean name followed by [redacted]@qq.com and "-270". A review of [redacted] records for [redacted]@qq.com identified a payment was sent to [redacted]@qq.com from [redacted] a China [redacted] account for $270 on May 8, 2020.

iii. According to [redacted] records, on or about July 20, 2021, the email address [redacted]@qq.com was provided to [redacted] user [redacted] from [redacted] requesting 250 be sent to the [redacted] account, [redacted]@qq.com. The user referred to [redacted] as "[redacted]", which your affiant knows to be a common North Korean

honorific. Based on review of Microsoft [redacted] records, the user [redacted] was subsequently identified as [redacted], an IT worker with Yanbian Silverstar. A review of [redacted] records for [redacted]@qq.com identified a $250 payment sent to [redacted]@qq.com from [redacted] account in the name of [redacted]. [redacted] sent a total of $52,400 to [redacted]@qq.com from June 2021 to September 2022.

iv. A review of open source information on December 6, 2022, identified a website for [redacted] which appeared to be a fake website purporting to work in geospatial development for the energy sector. The website did not have much content and did not have any pictures of their leadership or development team. According to the website, their offices are located in [redacted] but the company was registered as [redacted], LLC, in [redacted] The names may have been obtained from another website or an individual may have been recruited to create the company. A review of [redacted] for the profile of [redacted] identified 4 employees, one of who was "[redacted]". The picture on the [redacted] profile for [redacted] did not match the picture of [redacted] [redacted] profile which had been provided by the customer to [redacted] for verification purposes. Additionally, [redacted] [redacted] account identified their username as [redacted]" and indicated they were in Yanji, China and are native Korean. The use of three initials and "star" has been observed previously and

Yanji, China, is the location for Yanbian Silverstar. Both [redacted] and another company called [redacted] sent money to this [redacted] account.

v. North Korean IT workers create fake software development companies and include a basic website and [redacted] profile. They provide these to potential clients for verification purposes. Payments they receive from development are often sent to other [redacted] accounts they control. The money is then sent to other accounts to be withdrawn to Chinese bank accounts controlled by the group. There is probable cause to believe the account [redacted]@qq.com is an account controlled by North Koreans and used to transfer money for their IT work.

u. [redacted] Cardholder ID: 37224382 has an outstanding balance of $17,280.27 with the following account information:

Name: [redacted]

Registration Date: 04/12/2020

i. During the period of April 2020 to December 2022, the account received $787,385.10 from other [redacted] accounts, sent $1,369,963.97 to other [redacted] accounts, received $1,863,378.30 via ACH [redacted] and suspected freelancer jobs, paid $4,178.67 to job hiring and other online web sites, and withdrew a total of $1,377,791.32 to a bank account in

China.

ii. The [redacted] accoun[redacted]@126.com received multiple payments in a short time frame from other North Korean IT worker controlled accounts. For example, the [redacted] account [redacted]@gmail.com, which is discussed further below, sent four transactions totaling $22,830 from November 18 to November 30, 2022. On November 29, 2022, [redacted] account [redacted]@gmail.com, a **known IT worker controlled account,** sent $7,450. [redacted] using the [redacted] username [redacted] received a screenshot of the [redacted]@gmail.com [redacted] account from another unidentified North Korean. The transfer of large amounts over a short time to multiple North Korean IT worker controlled accounts demonstrates the [redacted] account [redacted]@126.com is controlled by North Korean IT workers.

v. [redacted] Cardholder ID: 36280506 has an outstanding balance of $4,343.62 with the following account information:

Name: [redacted]
Registration Date: 02/12/2020

i. During the period of June 2020 to April 2022, the account received $1,454,029.10 from other [redacted] accounts, sent $5,148 to other [redacted] accounts, and withdrew a total of $1,597,471 to a bank account in China.

ii. According to [redacted] records, in March 2020, the email address [redacted]@126.com and its password was shared between the two

[redacted] accounts controlled by [redacted], the Company President of Yanbian Silverstar, namely, [redacted] The sharing of the email and password demonstrates the account is controlled by North Korean IT workers.

w. [redacted] Cardholder ID: 15531742 has an outstanding balance of $3,967 with the following account information:

Name: [redacted]
Registration Date: 02/26/2016

i. During the period of September 2017 to December 2022, the account received $7,842,162.21 from other [redacted] accounts; sent $1,981,150.58 to other [redacted] accounts; received $17,423 via ACH from [redacted].com; received $4,235,530.65 via ACH from [redacted] and other sites; received $238,435.70 in suspected freelancer jobs from credit card payments; and withdrew a total of $9,961,754.34 to multiple bank accounts in China.

ii. According to the [redacted] there were 13 different China bank accounts associated to the [redacted] account, and 6 of those were in names other than [redacted]. The use of different China bank accounts in names other than the account holder has been seen frequently with North Korean IT worker accounts.

iii. A review of the documents provided by the customer to [redacted] identified a China National ID card whose ID number was the same one

provided for [redacted] account [redacted], [redacted]@qq.com, which is discussed above. Additionally, both accounts used the same screenshot of a [redacted] profile of [redacted], whose profile picture was taken from the China National ID submitted for [redacted]@outlook.com. Furthermore, the use of the same China National ID to open this account as another identified North Korean IT worker [redacted] account demonstrates both of these accounts are controlled by North Korean IT workers.

x. [redacted] Cardholder ID: 50966482 has an outstanding balance of $452.63 with the following account information:

Name: [redacted]
Registration Date: 03/13/2020

i. During the period of April 2022 to November 2022, the account received $186,512 from other [redacted] accounts, sent $37,345.65 to other [redacted] accounts, and withdrew a total of $132,245.00 to a bank account in China.

ii. According to records from Slack, the user with the email address [redacted]@gmail.com also operated the channel [redacted]slack.com, which identified multiple messages in Korean language from April 2022 to May 2022 where multiple North Korean Slack users listed the email address [redacted]@126.com followed by an amount. In March 2022, a user provided the email address and in Korean language indicated that other [redacted] accounts will deposit $500 a few times a week and then

the account could be used normally. This is a technique North Korean IT workers use to help verify and confirm the [redacted] account works before using it for larger deposits/withdrawals. This activity demonstrates that the email address [redacted]@126.com is used for North Korean IT work.

y. [redacted] Cardholder ID: 27500570 has an outstanding balance of $3,500 with the following account information:

Name: [redacted]

Registration Date: 07/22/2018

i. During the period of July 2018 to November 2022, the account received $253,084.56 from other [redacted] accounts, received $66,442.59 in payments from [redacted] and [redacted], and withdrew a total of $409,833.28 to a bank account in China.

ii. According to [redacted] records, in August 2018, the email address [redacted]@qq.com was shared by [redacted] user [redacted] to [redacted] which your affiant knows to be used by [redacted], Company President, Volasys Silver Star. In a message, the user [redacted] in Korean stated this was the '[redacted] account for '[redacted]s team". This demonstrates that the email address [redacted]@qq.com is used for North Korean IT work.

z. [redacted] Cardholder ID: 47739824 has an outstanding balance of $2,631.20 with the following account information:

Name: [redacted]

Registration Date: 11/03/2021

i. During the period of April 2022 to July 2022, the account received $64,125.89 from other [redacted] accounts, received $136,954.23 via ACH from various freelancer jobs, received $11,095 via third party credit cards for freelancer work, sent $151,164.46 to other [redacted] accounts, and withdrew a total of $64,220 to a bank account in China.

ii. The [redacted] account used the security answers "[redacted]", "[redacted]5", and "0120" which has been observed previously by North Korean controlled [redacted] accounts, specifically [redacted], the user of the [redacted] [redacted] account discussed above. Additionally, according to records from Microsoft, the name [redacted] was identified in [redacted] chats along with his date of birth and social security number. The name for [redacted] is redacted as this investigation has revealed that [redacted] is a victim of identity theft.

iii. A review of the documents provided by the customer to [redacted] identified a Spain National ID card with a picture of [redacted] Based on the picture and use of the [redacted] persona, the FBI believes the [redacted] address [redacted]@yahoo.com" is controlled by North Korean IT workers.

aa. [redacted] Cardholder ID: 36917596 has an outstanding balance of $2,789.14 with the following account information:

Name: [redacted]

Registration Date: 03/25/2020

i. During the period of April 2020 to July 2022, the account received $275,300.00 from [redacted] $129,715 from other [redacted] accounts, and sent $466,100 to other [redacted] accounts.

ii. The email account [redacted]@gmail.com was identified from a U.S. non-profit organization who had unknowingly hired a North Korean IT worker previously identified by the FBI as [redacted]. According to the FBI's investigation, [redacted] had recruited an individual from Belgium and used their identity to obtain a freelancer job from [redacted] After the FBI notified the non-profit organization of [redacted] fraud, the non-profit organization provided three additional freelancers whom they hired with similar activity to [redacted]. For example, each individual did not want to appear on camera, did not provide a picture for non-profit's website, and their [redacted] accounts got suspended. One of these individuals used the name [redacted] and email address [redacted]@gmail.com. They were paid through [redacted]

iii. Based on the use of the same email address, the FBI has probable cause to believe the [redacted] account is controlled by a North Korean IT worker who used a Ukrainian identity for their freelancer activity.

bb. [redacted]r Cardholder ID: 39386453 has an outstanding balance of $1,726.96 with the following account information:

Name: [redacted]

Registration Date: 08/10/2020

i. During the period of December 2020 to November 2022, the account received $199,529.96 from other [redacted] accounts, received $65,580.00 from [redacted], sent $250,161.00 to other [redacted] accounts, and withdrew a total of $103,100.00 to a bank account in China.

ii. According to records from Slack, the user with the email address [redacted]@gmail.com also operated the channel [redacted] slack.com, which identified multiple messages in Korean language from August 2021 to February 2022 where multiple North Korean Slack users listed the email address [redacted]@163.com followed by an amount. Some of the messages contained the words "Payment for React Native" and "Monthly payment for Java Project".

iii. In another Slack group called [redacted] slack.com, known to be operated IT workers, which contains multiple Korean-language communications about freelance IT work, a North Korean IT worker listed a [redacted] payment of $5,000 on August 24, 2021, for [redacted]@163.com. A review of [redacted] records for [redacted]@163.com identified a payment of $5,000 on August 24, 2021, was received from [redacted] account [redacted]", the contents of this [redacted] account were previously seized by the FBI pursuant to a federal seizure warrant in October 2022.

iv. According to [redacted] records, in August 2021, the email address [redacted]@163.com was shared by [redacted] user [redacted], used by [redacted] Delegation Leader, Yanbian Silverstar, to [redacted],

[redacted] Group Leader, Yanbian Silverstar, and they asked if the email address [redacted]@163.com was used by "[redacted]". [redacted] replied "yes." The FBI believes this was one North Korean asking about a different North Korean IT worker team's [redacted] account.

v. The payments requested and the discussion of the account in a North Korean Slack channel demonstrates that the email address [redacted]@163.com is controlled by North Korean IT workers.

cc. [redacted] Cardholder ID: 42171940 has an outstanding balance of $2,140 with the following account information:

Name: [redacted]
Registration Date: 01/25/2021

i. During the period from November 2022 to December 2022, the account received $2,902.57 via third party credit cards for freelancer work and withdrew a total of $679 to a bank account in China.

ii. According to [redacted] records, on or about March 21, 2021, [redacted] user [redacted] used by [redacted], a Delegation Leader for Yanbian Silverstar, requested [redacted], used by [redacted], the Company President of Yanbian Silverstar, to send money to a China bank account number [redacted] so he could pay a bill. The bank account was associated to the [redacted] account [redacted]@qq.com. The sharing of the china bank account number demonstrates the account is

controlled by North Korean IT workers.

dd. [redacted] Cardholder ID: 32872372 has an outstanding balance of $473.13 with the following account information:

Name: [redacted]
Registration Date: 07/19/2019

i. During the period of August 2019 to November 2022, the account received $156,205.38 from other [redacted] received $554,300.59 via ACH from [redacted] and other companies for freelancer work, sent $900,181.74 to other [redacted] accounts, and withdrew a total of $30,000 to a bank account in China.

ii. According to [redacted] records, in July 2020, the email address [redacted]@126.com and its password was shared between the two [redacted] accounts controlled by [redacted] the Company President of Yanbian Silverstar, namely, [redacted] The sharing of the email and password demonstrates the account is controlled by North Korean IT workers.

iii. A review of the documents provided by the customer to [redacted] show that the user claimed the domain hongshenguo.com as their website on or about August 8, 2019. According to [redacted] records, on or about August 9, 2019, [redacted] using the [redacted] username [redacted] received the domain hongshenguo.com from [redacted] user [redacted] used by [redacted] Delegation Leader for Yanbian Silverstar. [redacted] requested [redacted] create additional portfolio websites. North Korean

IT workers create websites for their IT worker personas in order to submit it to clients and for verification purposes for freelancer sites. There is probable cause to believe the domain hongshenguo.com is used for that purpose.

ee. [redacted] Cardholder ID: 46171038 has an outstanding balance of $3,189.85 with the following account information:

Name: [redacted]
Registration Date: 08/15/2021

i. During the period of August 2021 to November 2022, the account received $56,882.89 from other [redacted] accounts, received $37,102.19 via ACH from companies for freelancer work, received $31,430.24 via third party credit cards for freelancer work, sent $63,052.03 to other [redacted] accounts, and withdrew a total of $58,942.18 to a bank account in China.

ii. According to records from Slack, the user with the email address [redacted]@gmail.com also operated the channel [redacted]slack.com, which identified a message on April 25, 2022, from [redacted] requesting a payment of $3,100 be sent to [redacted]@163.com for "Monthly Payment for Python project". A screen shot of the [redacted] transaction was sent in response by [redacted] A review of the [redacted] records identified a payment was sent on April 25, 2022, from

[redacted] account [redacted], [redacted] a suspected North Korean IT worker account. No additional payments were sent from this account.

iii. A review of the documents provided by the customer to [redacted] shows several work invoices with the email address [redacted]@163.com, but instead of the Chinese name for the user it listed a Ukrainian name, address, and ID number. This information is not found anywhere in the registration for the [redacted] account. There is probable cause to believe the invoice was fraudulent in an effort to get the account verified by [redacted]

iv. The above activity corroborates the email address [redacted]@163.com is used by North Korean IT workers.

ff. [redacted] Cardholder ID: 27150482 has an outstanding balance of $1,529.52 with the following account information:

Name: [redacted]
Registration Date: 06/27/2018

i. During the period of April 2020 to November 2022, the account received $89,069.18 from other [redacted] accounts, sent $335,600.25 to other [redacted] accounts, received $518,242.02 via ACH from [redacted] and withdrew a total of $270,577.43 to bank accounts in China

ii. The [redacted] account [redacted]@yandex.com received a payment of $7,400 on November 18, 2022, from [redacted] account [redacted]@gmail.com, which is discussed below. Additionally,

the account received a payment of $1,000 on March 7, 2021, from [redacted] account "[redacted]". The contents of this [redacted] account were previously seized by the FBI pursuant to a federal seizure warrant in October 2022.

iii. A review of documents provided by the customer to [redacted] shows a screenshot of [redacted] transactions regarding payments the customer had received. Two payments for "[redacted]" were listed for August 26 and 28, 2021. According to [redacted] records, in June 2021, the user [redacted] shared the name "[redacted]" with [redacted], used by [redacted] a Delegation Leader for Yanbian Silverstar, who stated in Korean they believed the company belonged to a team in Dalian (China). The FBI believes the [redacted] user [redacted] was referring to another North Korean IT worker team based in Dalian, China. Based on the sharing of the [redacted] transactions in the name of a North Korean IT worker company name, your affiant believes that there is probable cause that the [redacted] account [redacted]@yandex.com is controlled by North Korean IT workers.

gg. [redacted] Cardholder ID: 42401507 has an outstanding balance of $154.99 with the following account information:

Name: [redacted]
Registration Date: 02/08/2021

i. During the period of March 2021 to November 2022, the account received $12,705.16 from other [redacted] accounts, received $16,910.00 via

[redacted], received $173,565.17 via ACH for freelancer work, sent $295,821.41 to other [redacted] and withdrew a total of $61,659.79 to a bank account in China. The account had two additional bank accounts in Ukraine but there were no withdrawals. Based on the foregoing, the FBI believes the account was created by a Ukrainian and then provided to a North Korean IT worker who added a bank in China on April 30, 2022.

ii. According to [redacted] records, in May 2021, the name, [redacted], email address, [redacted]@gmail.com, and specific ACH banking details, a date of birth, and address were shared between two North Korean IT workers. The two [redacted] accounts were identified as North Korean IT workers based on their communication regarding IT work, use of Korean language, and references to North Korea. The [redacted] user [redacted] sent [redacted] information to [redacted] user [redacted] Both actors work on behalf of Yanbian Silverstar. This demonstrates that the [redacted] account is controlled by North Korean IT workers.

hh. [redacted] Cardholder ID: 42171486 has an outstanding balance of $1,176.40 with the following account information:

Name: [redacted]

Registration Date: 01/25/2021

i. During the period of February 2021 to January 2022, the account sent $17,818.40 to other [redacted] accounts, and withdrew a total of $16,642 to

a bank account in China.

ii. According to [redacted] records, one of the bank accounts associated to the account was a China bank account ending in #9690. According to [redacted] records from Microsoft, on or about May 28, 2022, the bank account ending in #9690 was shared between the two [redacted] accounts controlled by [redacted] the Company President of Yanbian Silverstar, namely, [redacted]. The sharing of the bank account associated with the [redacted] account corroborates the [redacted] [redacted]@qq.com is controlled by North Korean IT workers.

ii. [redacted] Cardholder ID: 42654210 has an outstanding balance of $753.58 with the following account information:

Name: [redacted]
Registration Date: 02/24/2021

i. During the period of August 2021 to October 2022, the account received $293,544.48 from other [redacted] accounts, sent $47,138.87 to other [redacted] accounts, received $1,400 via ACH from [redacted] and withdrew $245,139.35 to bank accounts in China.

ii. According to [redacted] records, there were 7 bank accounts associated to the account, 4 or which were China bank accounts. One of the China bank accounts ends in #1678. According to [redacted] records from Microsoft, on or about February 22, 2019, the bank account ending in #1678 was shared between the [redacted] account [redacted] used by [redacted] the Representative/CEO of Yanbian Silverstar and [redacted]

used by [redacted], a Delegation Leader for Yanbian Silverstar. The sharing of the bank account associated with the [redacted] account corroborates the [redacted] account [redacted]@gmail.com is controlled by North Korean IT workers.

SEIZURE PROCEDURE FOR TARGET ACCOUNTS

43. The foregoing establishes probable cause to believe that the funds held in the **Target Accounts** are subject to civil and criminal forfeiture because those accounts and the funds within them were obtained through illegal employment by North Korean IT Workers in violation of U.S. sanctions, and were involved in a money laundering conspiracy.

44. Should this seizure warrant be granted, law enforcement intends to work with [redacted] to seize the funds contained within the **Target Accounts** by transferring the funds to a U.S. government-controlled account.

45. The seized currency in the **Target Accounts** will remain at the government-controlled account pending transfer of all right, title, and interest in the forfeitable property in the **Target Accounts** to the United States upon completion of forfeiture proceedings, to ensure that access to or manipulation of the forfeitable property cannot be made absent court order or, if forfeited to the United States, without prior consultation by the United States.

CONCLUSION

46. Based on the information contained herein and my training and experience, I submit that the **Target Accounts** are subject to seizure and forfeiture, pursuant to the above-referenced statutes. Based on the foregoing, I request that the Court issue the proposed seizure warrant.

47. Because Attachment A will be served on Payment Service Provider 1, which currently holds the associated funds, and thereafter, at a time convenient to it, will transfer the funds to the U.S. government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge.

[redacted]
Special Agent
Federal Bureau of Investigation

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 on this [redacted] day of January, 2023.

[redacted]
HONORABLE SHIRLEY P. MENSAH
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
PROPERTY TO BE SEIZED

Pursuant to this warrant, federal law enforcement agents are authorized to effectuate the seizure of all money, funds, and financial instruments deposited or credited to the below identified properties (the "**Target Accounts**") by serving this warrant on [redacted]

	Cardholder ID	Email	Registration Date	Amount
1	34661348	[redacted]	10/29/19	$60,000.00
2	48539184		12/9/21	$50,876.63
3	40408285		10/12/20	$182.00
4	38065868		5/28/20	$37,368.93
5	47630229		10/27/21	$33,024.13
6	42388706		2/7/21	$23,920.60
7	23163213		8/10/17	$19,018.68
8	56502641		8/9/22	$18,075.00
9	47779486		11/4/21	$17,431.24
10	53718284		6/13/22	$14,031.76
11	48542914		12/10/21	$11,221.10
12	44911814		6/21/21	$10,000.00
13	27185130		6/29/18	$9,130.00
14	52324106		5/2/22	$2,259.62
15	32838551		7/16/19	$7,232.86
16	48724076		12/20/21	$9,740.52
17	39841566		9/8/20	$14,881.76
18	42231644		1/29/21	$6,444.32
19	36782803		3/16/20	$6,398.23
20	31740755		4/23/19	$328.65
21	37224382		4/12/20	$17,280.27
22	36280506		2/12/20	$4,343.62
23	15531742		2/26/16	$3,967.00
24	50966482		3/13/22	$452.63
25	27500570		7/22/18	$3,500.00
26	47739824		11/3/21	$2,631.20
27	36917596		3/25/20	$2,789.14

28	39386453	[redacted]	8/10/20	$1,726.96
29	42171940		1/25/21	$2,140.00
30	32872372		7/18/19	$473.13
31	46171038		8/15/21	$3,189.85
32	27150482		6/27/18	$1,529.52
33	42401507		2/8/21	$154.99
34	42171486		1/25/21	$1,176.40
35	42654210		2/24/21	$753.58

TOTAL: $397,674.32